UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	CASE NO. CR19-00159-RSL
Plaintiff,	)	
	)	Seattle, Washington
v.	)	
	)	June 16, 2022
PAIGE A. THOMPSON,	)	9:00 a.m.
	)	
Defendant.	)	JURY TRIAL, Vol. 8 of 9
	)	

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 98101

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy L. Bauer, CRR, RPR
Marci Chatelain, CRR, RPR, RMP, CCR
Official Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
nancy_bauer@wawd.uscourts.gov

INDEX

PROCEEDINGS

THE COURT: Mr. Klein, you had something you wanted to add to the exceptions to the Court's instructions given and not given?

MR. KLEIN: Yes, Your Honor.

We had three more formal exceptions. They are from Docket No. 286, which was our initial proposal of jury instructions, and they're Defendant's Requested Instructions 8, 9, and 10. No. 8 deals with trade secrets; No. 9 deals with independent economic value; and No. 10 deals with the secrecy, with the maintaining secrecy.

THE COURT: Okay. Those are noted for the record, and the Court will stay with the instructions as proposed yesterday.

Anything else before we bring the jury in? Mr. Friedman, all set?

MR. FRIEDMAN: Yes, Your Honor.

THE COURT: And, Mr. Hamoudi, all set?

MR. HAMOUDI: We're all set, Your Honor.

THE COURT: Great. Victoria will bring the jury in.

(Brief pause in proceedings.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Thank you, please be seated.

As promised, on your chairs, instead of the notebooks, is

the Court's instructions to the jury, and a pen.

Why don't you all write your juror numbers on those, and those will stay with you when you are in the jury room. You'll leave them on your chairs when we're done here, and Victoria will bring them back to you.

So your copies of the Court's instructions have my signature in black. The original, which the presiding jury will hold on to, my signature is in blue ink, and only write on the originals to fill out the verdict form.

You can take notes on the copies, and they will either be destroyed at the end of the case, or given to you as a door prize for your wonderful participation.

So the Court's instructions represent the best effort of me, with the assistance of counsel, to provide you with the law you need to decide the case.

Where specific legal terms are used, they are defined for you in these instructions. If there is no specific legal definition, use common, everyday meaning to define words. But under no circumstances should you consult any outside sources of information. I used to say, "Don't ask Jeeves," but nobody even knows what that was anymore. But don't do any Google searches or any law searches or anything like that. Everything you need to know about the case is in these Court's instructions to the jury, which I'm going to read to you now.

Instruction No. 1: Members of the jury, now that you have

heard all the evidence, it is my duty to instruct you on the law that applies to this case. A copy of these jury instructions will be available in the jury room for you to consult.

It is your duty to weigh and evaluate all the evidence received in the case, and in that process to decide the facts. It is also your duty to apply the law as I give it to you to the facts as you find them, whether you agree with the law or not. You must decide the case solely on the evidence and the law. You will recall you took an oath promising to do so at the beginning of the case.

You should also not been influenced by any person's race, color, religious beliefs, national ancestry, sexual orientation, gender identity, gender, or economic circumstances. Also, do not allow yourself to be influenced by personal likes or dislikes, sympathy, prejudice, fear, public opinion or biases, including unconscious biases.

Unconscious biases are stereotypes, attitudes, or preferences that people may consciously reject, but may be expressed without conscious awareness, control, or intention.

You must follow all these instructions and not single out some and ignore others. They are all important. Please do not read into these instructions, or into anything I may have said or done, any suggestion as to what verdict you should return. That is a matter entirely up to you.

The indictment is not evidence. The defendant has pleaded

not guilty to the charges. The defendant is presumed to be innocent unless and until the government proves the defendant guilty beyond a reasonable doubt.

In addition, the defendant does not have to testify or present any evidence. The defendant does not have to prove innocence. The government has the burden of proving every element of the charges beyond a reasonable doubt.

A defendant in a criminal case has a constitutional right not to testify. In arriving at your verdict, the law prohibits you from considering, in any manner, that defendant did not testify.

Proof beyond a reasonable doubt is proof that leaves you firmly convinced the defendant is guilty. It is not required that the government prove guilt beyond all possible doubt. A reasonable doubt is a doubt based upon reason and common sense, and is not based purely on speculation. It may arise from a careful and impartial consideration of all the evidence, or from lack of evidence.

If, after a careful and impartial consideration of all the evidence, you are not convinced beyond a reasonable doubt that the defendant is guilty, it is your duty to find the defendant not guilty. On the other hand, if, after a careful and impartial consideration of all the evidence, you are convinced beyond a reasonable doubt that the defendant is guilty, it is your duty to find the defendant guilty.

The parties have agreed to certain facts that have been stated to you. Those facts are now conclusively established.

The evidence you are to consider in deciding what the facts are consists of, first, the sworn testimony of any witness, second, the exhibits received in evidence, and third, any facts to which the parties have agreed.

No. 7: In reaching your verdict, you may consider only the testimony and exhibits received in evidence. The following things are not evidence and you may not consider them in deciding what the facts are:

Questions, statements, objections, and arguments by the lawyers are not evidence. The lawyers are not witnesses. Although you must consider a lawyer's questions to understand the answers of a witness, the lawyers' questions are not evidence.

Similarly, what the lawyers have said in their opening statements and will say in their closing arguments and have said at other times is intended to help you interpret the evidence, but it is not evidence. If the facts as you remember them differ from the way the lawyers state them, your memory of them controls.

Any testimony that I have excluded, stricken, or instructed you to disregard is not evidence. Anything you may have seen or heard when court was not in session is not evidence. You are to decide the case solely on the evidence received at trial.

Evidence may be direct or circumstantial. Direct evidence is direct proof of a fact, such as testimony by a witness about what that witness personally saw or heard or did. Circumstantial evidence is indirect evidence. That is, it is proof of one or more facts from which you can find another fact. You are to consider both direct and circumstantial evidence. Either can be used to prove any fact. The law makes no distinction between the weight to be given to either direct or circumstantial evidence. It is for you to decide how much weight to give to any evidence.

No. 9: In deciding the facts in this case, you may have to decide which testimony to believe and which testimony not to believe. You may believe everything a witness says, part of it, or none of it.

In considering the testimony of any witness, you may take into account the following:

First, the opportunity and ability of the witness to see or hear or know the things testified to; second, the witness's memory; third, the witness's manner while testifying; fourth, the witness's interest in the outcome of the case, if any; fifth, the witness's bias or prejudice, if any; six, whether other evidence contradicted the witness's testimony; seven, the reasonableness of the witness's testimony in light of all the evidence; and eight, any other factors that bear on believability.

Sometimes a witness may say something that is not consistent with something else he or she said. Sometimes different witnesses will give different versions of what happened. People often forget things and make mistakes in what they remember. Also, two people may see the same event but remember it differently.

You may consider these differences, but do not decide that testimony is untrue just because it differs from other testimony.

However, if you decide that a witness has deliberately testified untruthfully about something important, you may choose not to believe anything that witness said; on the other hand, if you think the witness testified untruthfully about some things but told the truth about others, you may accept the part you think is true, and ignore the rest.

The weight of the evidence as to a fact does not necessarily depend on the number of witnesses who testify. What is important is how believable the witnesses were and how much weight you think their testimony deserves.

These factors apply equally to the testimony of law enforcement witnesses. Their testimony is to be given no extra consideration or weight. You are to evaluate and treat their testimony like you would any other witness.

You are here only to determine whether the defendant is guilty or not guilty of the charges in the indictment. The

defendant is not on trial for any conduct or offense not charged in the indictment.

No. 11: A separate crime is charged against the defendant in each count. You must decide each count separately. Your verdict on one count should not control your verdict on any other count.

The indictment charges that offenses alleged in Counts 1, 2, 4, 5, 6, 7, 9, and 10, were committed on or about certain dates. The indictment charges that the offense alleged in Count 8 was committed on or before and on or after certain dates.

Although it is necessary for the government to prove beyond a reasonable doubt that the offenses were committed on dates reasonably near the dates alleged in Counts 1, 2, and 4 through 10 of the indictment, it is not necessary for the government to prove that the offenses were committed precisely on the dates charged.

And, remember, we dismissed, on the motion of the government, Count 3, which is why we go "1, 2, 4." There is no Count 3 in front of you.

No. 13: You have heard testimony that the defendant made statements. It is for you to decide whether the defendant made the statements, and, if so, how much weight to give to them.

In making those decisions, you should consider all the evidence about the statements, including the circumstances under

which the defendant may have made them.

You have heard evidence that the defendant committed other acts not charged here. You may consider this evidence only for its bearing, if any, on the question of the defendant's intent, motive, opportunity, preparation, plan, knowledge, identity, absence of mistake, absence of accident, and for no other purpose.

No. 15: You have heard testimony from persons who testified to opinions and the reasons for their opinions. This opinion testimony is allowed because of the education or experience of these witnesses.

Such opinion testimony should be judged like any other testimony. You may accept it or reject it, and give it as much weight as you think it deserves, considering the witness's education and experience, the reasons given for the opinion, and all the other evidence in the case.

During the trial, charts and summaries were shown to you to help explain the evidence in the case. Certain charts and summaries have been admitted into evidence. Charts and summaries are only as good as the underlying supporting material. You should, therefore, give them only such weight as you think the underlying material deserves.

Other charts and summaries were not admitted into evidence and will not go into the jury room with you. These were for illustrative purposes only. They are not themselves evidence or

proof of any facts. If they do not correctly reflect the facts or figures shown by the evidence in the case, you should disregard these charts and summaries, and determine the facts from the underlying evidence.

No. 17: The defendant is charged in Count 1 of the indictment with wire fraud, in violation of Section 1343 of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, beginning on or before March 2019, and continuing until on or about July 17 of 2019, the defendant knowingly devised and intended to devise a scheme or plan to defraud or a scheme or plan for obtaining money or property from the one who is deceived by means of false or fraudulent pretenses, representations, or promise;

Second, the statements made as part of the scheme were material; that is, they had a natural tendency to influence or were capable of influencing a person to part with money or property;

Third, the defendant acted with intent to defraud;

And fourth, on or about March 22, 2019, the defendant used or caused to be used an interstate or foreign wire communication to carry out an essential part of the scheme.

An act is done knowingly if the defendant is aware of the act and does not act through ignorance, mistake, or accident.

The government is not required to prove that the defendant knew that her acts or omissions were unlawful. You may consider evidence of the defendant's words, acts, or omissions, along with all the other evidence, in deciding whether the defendant acted knowingly.

In determining whether a scheme to defraud exists, you may consider not only the defendant's words and statements, but also the circumstances in which they are used as a whole.

An intent to defraud is an intent to deceive and cheat; that is, an intent to deprive a victim of money or property by deception.

A wiring is caused when one knows that a wire will be used in the ordinary course of business, or when one can reasonably foresee such use. It need not be reasonably foreseeable to the defendant that the wire communication would be interstate or foreign in nature; rather, it must have been reasonably foreseeable to the defendant that some wire communication would occur in furtherance of the scheme, and an interstate or foreign wire communication must have actually occurred in furtherance of the scheme.

The defendant is charged in Count 2 of the indictment with unlawfully obtaining information of Capital One, in violation of Section 1030(a)(2) of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable

doubt:

First, between on or about March 12, 2019, and on or about July 17 of 2019, the defendant intentionally accessed, without authorization, a computer;

Second, by accessing without authorization a computer, the defendant obtained information contained in a financial record of a card issuer;

And third, the value of the information obtained exceeded $5,000.

A person accesses a computer without authorization when, one, the computer is protected by a generally applicable rule regarding access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer; and two, the person circumvents that rule regarding access permissions to gain access to the computer.

The term "card issuer" means any person who issues a credit card, or the agent of such person with respect to such card.

No. 19: The defendant is charged in Count 4 of the indictment with unlawfully obtaining information from Apperian's protected computer, in violation of Section 1030(a)(2) of Title 18 of the United States Code.

For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, on or about March 7, 2019, the defendant intentionally accessed, without authorization, Apperian's computer; and second, by accessing without authorization Apperian's computer, the defendant obtained information from a computer that was used in or affecting interstate or foreign commerce or communication; and third, the value of the information obtained exceeded $5,000.

A person accesses a computer, quote, without authorization, when the computer is protected by a generally applicable rule regarding access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer, and the person circumvents that rule regarding access permissions to gain access to the computer.

The defendant is charged in Count 5 of the indictment with unlawfully obtaining information from Survox's protected computer, in violation of Section 1030(a)(2) of Title 18 of the United States Code.

For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, on or about March 12, 2019, the defendant intentionally accessed, without authorization, Survox's computer; and second, by accessing without authorization Survox's computer, the defendant obtained information from a

computer that was used in or affecting interstate or foreign commerce or communication; and third, the value of the information obtained exceeded $5,000.

A person accesses a computer without authorization when a computer is protected by a generally applicable rule regarding access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer, and the person circumvents that rule regarding access permissions to gain access to the computer.

No. 21: The defendant is charged in Count 6 of the indictment with unlawfully obtaining information from Bitglass's protected computer, in violation of 1030(a)(2) of Title 18 of the United States Code.

For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, on or about March 5, 2019, the defendant intentionally accessed, without authorization, Bitglass's computer; and second, by accessing without authorization Bitglass's computer, the defendant obtained information from a computer that was used in or affecting interstate or foreign commerce or communications.

A person accesses a computer without authorization when the computer is protected by a generally applicable rule regarding

access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer, and the person circumvents that rule regarding access permissions to gain access to the computer.

The defendant is charged in Count 7 of the indictment with unlawfully obtaining information from 42Lines' protected computer, in violation of 1030(a)(2) of Title 18 of the United States Code.

For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, on or about March 28, 2019, the defendant intentionally accessed, without authorization, 42Lines' computer; and second, by accessing, without authorization, 42Lines' computer, the defendant obtained information from a computer that was used in or affecting interstate or foreign commerce or communication.

A person accesses a computer without authorization when the computer is protected by a generally applicable rule regarding access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer, and the person circumvents that rule regarding access permission to gain access to the computer.

No. 23: The defendant is charged in Count 8 of the indictment with transmitting a program information code or command to a computer intending to cause damage, in violation of Section 1030(a)(5) of Title 18 of the United States Code.

For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, beginning on or about March 10, 2019, and continuing until on or after August 5, 2019, the defendant knowingly caused the transmission of a program, information code, or command to a computer;

Second, as a result of the transmission, the defendant intentionally impaired, without authorization, the integrity or availability of data, a program, a system, or information;

Third, the computer was used in or affected interstate or foreign commerce or communication;

And fourth, the offense caused loss to one or more persons during a one-year period, including loss from a related course of conduct, aggregating at least $5,000 in value.

An act is done knowingly if the defendant is aware of the act and does not act through ignorance, mistake, or accident. The government is not required to prove that the defendant knew her acts or omissions were unlawful. You may consider evidence of the defendant's acts or omissions, along with all the other evidence, in deciding whether the defendant acted knowingly.

The term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

For purposes of Counts 4, 5, 6, 7, and 8, a computer is used in or affecting interstate or foreign commerce or communication if it is connected to the Internet.

No. 25: The defendant is charged in Count 9 of the indictment of unlawful possession and attempted unlawful possession of unauthorized access devices, in violation of Section 1029(a)(3) of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt;

First, beginning on or about March 12, 2019, and continuing until on or about July 17, 2019, the defendant knowingly possessed or attempted to possess at least 15 unauthorized access devices at the same time;

Second, the defendant knew that the devices were unauthorized;

Third, that the defendant acted with intent to defraud;

And fourth, the defendant's conduct, in some way, affected commerce between one state and another state or states, or between a state of the United States and a foreign country.

An act is done knowingly if the defendant is aware of the act, and does not act through ignorance, mistakes, or accident.

The government is not required to prove that the defendant knew that her acts or omissions were unlawful. You may consider evidence of the defendant's words, acts, or omissions, along with all the other evidence, in deciding whether the defendant acted knowingly.

A person has possession of something if the person knows of its presence and has physical control of it, or knows of its presence and has the power and intention to control it.

A defendant attempts to commit a crime when she intends to commit the crime, and she does something that is a substantial step toward committing the crime, and it strongly corroborates her intent to commit the crime.

Mere preparation is not a substantial step toward committing the crime. To constitute a substantial step, a defendant's act or actions must unequivocally demonstrate that the crime will take place unless interrupted by independent circumstances.

Jurors do not need to agree unanimously as to which particular act or actions constituted a substantial step toward the commission of a crime.

An access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used alone or in conjunction with

another access device to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument.

An "unauthorized access device" means any access device that is lost, stolen, expired, revoked, cancelled, or obtained with the intent to defraud. An intent to defraud is an intent to deceive and cheat; that is, an intent to deprive a victim of money or property by deception.

The defendant is charged in Count 10 of the indictment with aggravated identity theft, in violation of Section 1028(A)(a)(1) of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, beginning on or about March 12, 2019, and continuing until on or about July 17, 2019, the defendant knowingly possessed, without legal authority, a means of identification of another person;

Second, the defendant knew that the means of identification belonged to a real person;

And third, the defendant did so during and in relation to access device fraud, as charged in Count 9.

An act is done knowingly if the defendant is aware of an act and does not act through ignorance, mistake, or accident. The government is not required to prove that the defendant knew

that her acts or omissions were unlawful. You may consider evidence of the defendant's words, acts, or omissions, along with all the other evidence, in deciding whether the defendant acted knowingly.

The term "means of identification" means any name or number that may be used alone or in conjunction with any other information to identify a specific individual. The term includes any name, Social Security number, or date of birth.

No. 27: When you begin your deliberations, elect one member of the jury as your presiding juror who will preside over the deliberations and speak for you here in court.

You will then discuss the case with your fellow jurors to reach agreement, if you can do so. Your verdict, whether guilty or not guilty, must be unanimous.

Each of you must decide the case for yourself, but you should do so only after you have considered all the evidence, discussed it fully with the other jurors, and listened to the views of your fellow jurors.

Do not be afraid to change your opinion if the discussion persuades you that you should, but do not come to a decision simply because other jurors think it is right.

It is important that you attempt to reach a unanimous verdict, but, of course, only if each of you can do so after having made your own conscientious decision.

Do not change an honest belief about the weight and effect

of the evidence simply to reach a verdict.

Perform these duties fairly and impartially. You should also not be influenced by any person's race, color, religious beliefs, national ancestry, sexual orientation, gender identity, gender, or economic circumstances. Also, do not allow yourself to be influenced by personal likes or dislikes, sympathy, prejudice, fear, public opinion, or biases, including unconscious biases. Unconscious biases are stereotypes, attitudes, or preferences that people may consciously reject, but may be expressed without conscious awareness, control, or intention.

It is your duty as jurors to consult with one another and to deliberate with one another with a view towards reaching an agreement, if you can do so. During your deliberations, you should not hesitate to reexamine your own views and change your opinion if you become persuaded that it is wrong.

Because you must base your verdict only on the evidence received in the case and on these instructions, I remind you that you must not be exposed to any other information about the case or the issues it involves.

Except for discussing the case with your fellow jurors during your deliberations, do not communicate with anyone in any way, and do not let anyone else communicate with you in any way about the merits of the case or anything to do with it. This restriction includes discussing the case in person, in writing,

by phone, tablet, computer, or any other means, by email, text message, or any Internet chat room, blog, website, or any other form of social media.

This restriction applies to communicating with your family members, your employer, the media, the press, and the people involved in the trial. If you are asked or approached in any way about your jury service or anything about this case, you must respond you have been ordered not to discuss the matter, and report this contact to the Court.

Do not read, watch, or listen to any news or media accounts or commentary about the case or anything to do with it. Do not do any research such as consulting dictionaries, searching the Internet, or using other reference materials, and do not make any investigation or in any other way try to learn about the case on your own.

The law requires these restrictions to ensure the parties have a fair trial based upon the same evidence that each party has had an opportunity to address. A juror who violates these restrictions jeopardizes the fairness of these proceedings, and a mistrial could result that would require the entire trial process to start over.

If any juror is exposed to any outside information, please notify the Court immediately.

No. 29: Some of you have taken notes during the trial. Whether or not you took notes, you should rely on your own

memory of what was said. Notes are only to assist your memory, and you should not be overly influenced by your notes or those of your fellow jurors.

Those exhibits capable of being displayed electronically will be provided to you in that form, and you will be able to view them in the jury room. A computer, projector, and accessory equipment will be available for you in the jury room.

A court technician -- that is Victoria -- will show you how to operate the computer and other equipment, how to locate and view the exhibits on the computer. You will also be provided with a paper list of all the exhibits received in evidence. You may request a paper copy of an exhibit received in evidence by sending a note through the clerk, Victoria. If you need additional equipment or supplies, you can make such a request by sending a note.

In the event of any technical problem, or if you have questions about how to operate the computer or other equipment, send Victoria a note signed by the foreperson or by one or more members of the jury. Be as brief as possible in describing the problem, and do not refer to or discuss any exhibit you are attempting to view.

If a technical problem or question requires hands-on maintenance or instructions, a court technician may enter the jury room, with the clerk present, for the sole purpose of assuring that the only matter that is discussed is the technical

problem.

When the court technician or any non-juror is in the jury room, the jury shall not deliberate. No juror may say anything to the court technician or any non-juror, other than to describe the technical problem or seek information about operation of the equipment. Do not discuss any exhibit or any aspect of the case.

The sole purpose of providing this computer in the jury room is to enable jurors to view the exhibits received in evidence in this case. You may not use the computer for any other purposes. At my direction, the technicians have taken steps to make sure the computer does not permit access to the Internet or to any outside website, database, directory, game, or other material.

Do not attempt to alter the computer to obtain access to such materials. If you discover that the computer does provide or allow access to such materials, please inform us immediately, and refrain from using such materials. Do not remove the computer or any electronic data from the jury room, and do not copy any such data.

No. 31: The punishment provided by law for the crime here is for the Court to decide. You may not consider punishment in deciding whether the government has proved its case against the defendant beyond a reasonable doubt.

A verdict form has been prepared for you. All of the

verdict forms you have have "copy" stamped on them, just like the instructions do; the original does not. After you have reached unanimous agreement on the verdict, your presiding juror should complete the verdict form according to your deliberations, sign and date it, and advise the clerk that you are ready to return to court.

Final one, No. 33: If it becomes necessary during your deliberations to communicate with me, you may send a note, through the clerk, signed by any one or more of you. No member of the jury should ever attempt to communicate with me, except by a signed writing, and I will respond to the jury concerning the case only in writing or here in open court.

If you send out a question, I will consult with the lawyers before answering it, which may take some time. You may continue your deliberations while waiting for the answer to any question. Remember, you're not to tell anyone, including me, how the jury stands, numerically or otherwise, on any question submitted to you, including the question of the guilt of the defendant, until after you have reached a unanimous verdict or have been discharged.

So would you now please give your attention to Assistant United States Attorney Andrew Friedman, who will make the closing argument on behalf of the government.

Counsel?

GOVERNMENT'S CLOSING ARGUMENT

MR. FRIEDMAN: Good morning, ladies and gentlemen of the jury.

In the spring of 2019, Paige Thompson embarked on a massive hacking campaign against clients of AWS. She scammed tens of millions of addresses on the Internet, looking for firewalls that had been misconfigured. When she found vulnerabilities, she hacked into them, she stole credentials, and she used those credentials to steal as much data as she could, and to engage in cryptojacking; that is, mining cryptocurrency using other people's resources.

She knew what she was doing was illegal. She said that time and again. But she didn't care. She wanted the money that she got from cryptojacking, she wanted the data, and she wanted to brag and show other people that she was smarter than them. The one thing she didn't want was to help any of the victims whose computers she hacked into.

Ladies and gentlemen, evidence comes in in a trial in kind of an arbitrary manner. You hear from one witness after another. They each tell you about their part of the story, what they saw. And so what I want to do this morning is I want to spend a few minutes pulling some of that evidence together to show the overall picture, and then I want to talk about the crimes with which Ms. Thompson is charged, and how the evidence shows that she committed each of those crimes, and, finally, to

the extent I haven't already done so, I want to talk about some of the arguments that the defense has made during the course of this trial.

So let's start with the evidence.

Ladies and gentlemen of the jury, by now you're familiar with how Paige Thompson committed her hack. You know what's called her Attack Vector. She scanned tens of millions of AWS clients' computers looking for firewalls that had been configured in a way that allowed them to proxy or relay her messages to something called the Instance Metadata Service.

The Instance Metadata Service should never communicate with outside computers. It should not be able to communicate with them. But Ms. Thompson, when she found ones where the configuration allowed that, she asked a series of questions, looking for a series of pieces information: The ID of the computer, the AMID that she was talking to; roles that were available that she might be able to assume; and, ultimately, the credentials for those roles, the secret access key, the access key that she would be able to use if she had those roles.

Now, Ms. Thompson shouldn't have been able to communicate with the Instance Metadata Service, and it shouldn't have answered her questions, but it did because of how she had approached it, how she tricked it.

Remember Steve Schuster? He was a witness from AWS, the first witness to testify in the trial. That's the word he used

to describe what Ms. Thompson did. She tricked the hypervisor. She fooled the Instance Metadata Service into answering her question.

The Instance Metadata Service provided the information because it thought it was talking to the firewall. It thought the firewall was asking those questions, and so it provided the information, it provided role, it provided the access key, it provided the secret access key. And when the Instance Metadata Service provided that information to the firewall, the firewall relayed it on to Ms. Thompson, and once she had that information, she could go to the races.

With those credentials, she was able to access AWS's command line interface, use those credentials to enter victims' spaces, and do whatever those credentials had permission to do. If they had permission to read and copy data, she was able to read and copy that data. If they had permission to launch new virtual servers and instances, she could launch new instances, and she could place software on those instances to conduct cryptojacking, basically to mine cryptocurrency using the companies' resources for her own benefit.

Now, these diagrams make what Ms. Thompson did look relatively simple. But you've seen the code, and you know it's really not that simple. Ms. Thompson had found a vulnerability that no one else had found before.

And you remember Waymon Ho, the FBI computer scientist? As

he explained it to you, he looked at the code. He could see Ms. Thompson figuring out how to do this. He could see her code evolving over time. He could see her running into roadblocks, getting errors, and figuring a way around those. So this was a complicated process for her to figure out.

And, remember, Steve Schuster has been at Amazon doing cyber security for nearly ten years, and he told you that no one had ever succeeded in hacking into AWS from the outside, in this way, and stealing clients' information. This was a novel -- it was a complicated exploit. It was a vulnerability that Ms. Thompson found that others hadn't seen, and she figured out how to take advantage of.

And AWS, when they learned about the breach, they were worried about this for their other clients, and they actually performed a scan of the entire universe of their clients to see who else might have configured computers in this way, because it might well be a mistake, and informed all of those clients so they could protect themselves so they wouldn't be vulnerable to the same kind of hack.

Between March of 2019 and August of 2019, Ms. Thompson spent a lot of time working on this. She must have spent hundreds of hours on this exploit. And you have seen, through Mr. Ho's testimony, pieces of her computer that were devoted to that. File after file, folder after folder of scripts, of information relating to the results of running those scripts, of

information she got from AWS.

This is the beginning, the high-level folder. It's called "aws_hacking_shit." That's where Ms. Thompson put much of the information that she used in this hacking campaign, scripts that she used, responses, tools that she used in her campaign.

"aws_scanner," that's a folder that's filled with materials that she used as part of her scanning campaign looking for the vulnerability.

".aws," this is information that, once she had scanned, once she had found the vulnerability and got information, this is the information she used in order to communicate with AWS's command line interface, in order to enter the AWS environment, in order to proceed towards taking data, towards mining.

"aws_dumps," this is a folder with file -- with subfolders, one after another, containing information that Ms. Thompson stole from clients of AWS and that she stored on her computer. And you see the first few here, just the A's.

And "miner," this is a folder that had mining scripts, all of the tools that Ms. Thompson used in order to plant cryptocurrency mining software on victims' computers in order to cryptojack.

And Ms. Thompson, she was acting at almost industrial scale. This is a message that she sent. She's talking about how broad her scanner was, how much it scanned. She scanned 36 million addresses trying to find the relatively few who made a

mistake in how they configured their defenses. Her scanner took 20 hours to look at that universe.

And this is a bigger shot of the aws_dumps folder. Each one of these folders represents information stolen from a different client. More than 30 different victims, some of whom lost massive amounts of information. You've heard about Capital One, 100 million people's records, you've heard about Apperian, the company's entire source code and client database, all stored on Ms. Thompson's computer.

And Ms. Thompson was acting on the same scale in mining. This is a message exchange that resulted from her request to open new instances for cryptojacking. And the message here, basically, tells Ms. Thompson, "You've exceeded the quota of new instances you can open on this account. You've gone over your quota," and when I say "your quota," I really mean the victim client's quota, the account that she hacked into, because you as a client, you're only allowed 20 more instances, but you've asked for 100. She's trying to open 100 new computers, high-powered computers, to cryptojack.

And this is an excerpt from another file you saw. This is the "AWS commands" files. It has commands that Ms. Thompson saved because she thought they were of note, that they would be useful letter.

And the final command, you can see how long this is. This folder goes 64 pages when you look at it. The final line is

command 10,007. This was a full-time enterprise by Ms. Thompson during those months.

Now, based on Ms. Thompson's conduct, she's charged with nine crimes, and I want to start by talking about the crimes that charge unauthorized access to a computer, and those are Counts 2 and 4 through 7.

Each one of those counts is based on a different client, a different computer that she accessed. And each one of those counts requires the government to find several things. They all begin by asking the government to find that Ms. Thompson intentionally accessed a computer without authorization. So that's a common element between all of those. Because that's the longest discussion, I'm going to come back to that in a minute.

Each of them also requires the government to prove other things. So for Count 2, which relates to Capital One, the government has to prove that Ms. Thompson obtained information in a financial record of a card issuer. And you know that's true. Capital One is a credit-card-issuing business.

And Mike Fisk told you that the data that she obtained, the data in the folders that she took, was transaction data. So there is no question about that.

And third, the government has to prove that the value of the information exceeded $5,000. And, remember, Ken Henderson, the secret service agent, he came in and told you that the data

set that she took would probably be worth $500,000 or more. There's no question that it's worth more than $5,000 on the black market.

Counts 4 and 5, the two extra things the government has to prove in those counts -- and those counts relate to Apperian and Survox -- the government has to prove that the computer was used in or affecting interstate commerce. And you have, in your instructions, an instruction that says if the computer is connected to the Internet, it's used in or affecting interstate commerce, and so there is no question about that, these are computers of businesses connected to the Internet -- that's how Ms. Thompson got to them -- a business that acted in interstate commerce.

Third, for these two counts, the government has to prove that value of the information was more than $5,000, and, again, the evidence you heard shows there's no question for these two topics.

Remember Matt Pelaggi, who worked for Apperian? He told you that the information Ms. Thompson took was the company's entire source code for its product and its entire customer database; basically, the entire company. They had paid much more than that for it. It would cost far more than $5,000 to re-create. It not a close question.

In the case of Survox, remember John Roundy testified, and he said Ms. Thompson had taken more than a million customer

records, and he was confident that those were worth more than $100,000. So, again, there is no question that the value was over $5,000.

For the last two of these counts, Counts 6 and 7, which relate to Bitglass and 42Lines, the government has to prove the computer is connected to the Internet and, therefore, used in interstate commerce. Again, no question about that. That's the only additional element for those two counts.

So that brings us to, basically, the central issue here, which is, did Ms. Thompson access these computers without authorization? And the answer to that is clearly "yes."

Each of these counts includes a definition of "without authorization," and it's the same definition for all of them, so I'm just showing one. But it provides, "A person accesses a computer without authorization when the computer is protected by a generally applicable rule regarding access permissions, such as a username and password requirement, credential requirement, or other authentication system that prevents the general public from accessing the computer, and, two, the person circumvents that rule regarding access permissions to gain access to the computer."

The evidence in this case has shown that that's true.

The computers that Ms. Thompson accessed in order to steal data, in order to run new instances, were the internal environments of all these -- the internal AWS environments of

all these instances we've been talking about. She accessed that through the AWS command line interface. She did that using credentials, the credentials that she had stolen through the misconfigured firewall.

Now, the command line interface requires those credentials. Neither you nor I, we can't just log into one these companies' environments, because we don't have those credentials.

Ms. Thompson, a company who didn't know her, she didn't have those credentials and the ability to log-in there, and so those buckets, that environment is protected by credential requirement. That's the first part of this definition.

The second part is that the person has circumvented that rule. And Ms. Thompson circumvented that rule. She didn't have those credentials, but she obtained them by tricking the firewall to send a request on to the Instance Metadata Service, and by causing it, thinking it was answering the firewall, to provide those credentials to her.

So Ms. Thompson is not a person who should have had these credentials. She performed this trick, she got the credentials and she circumvented the general requirement.

And you can see that. This is the top of the gist that kind of brought this whole thing to light. This is Ms. Thompson's entry into Capital One's environment. And you can see that she is proxying through the Internet service -- the IP address that starts with 35.162, she's going to the Instance

Metadata Service, she's asking for the latest security credentials for Capital One. That's circumventing the way this is supposed to work. That is circumventing the general protection on going into the Capital One's AWS environment.

And ladies and gentlemen of the jury, stepping back a little bit, that makes sense. You know Ms. Thompson was not authorized by Capital One. Capital One didn't know who Ms. Thompson was before this started. They tell her, "Hey, come on into our environment. Make yourself comfortable. If you see some data, take it. If you want to mine cryptocurrency, go for it. Don't worry, we'll pick up the tab." That did not happen. That would never have happened.

What actually happened is, each of these companies had a security system in place. They had credential requirements. They required authentication in order to enter the environments. And you heard about that from each of the witnesses who testified.

Remember Chris Chan from Bitglass? He talked about how this was a sensitive environment, and if an employee wanted to go in there, they had to first log in to the company using a VPN, which required a multifactor authentication, and then from there, they had to log in to the environment, and that took an access key and more multifactor authentication.

So these were all environments that were protected by systems designed to exclude outsiders, systems that Ms. Thompson

circumvented.

And each of the witness companies was asked the question, like the question asked of Mr. Pelaggi: "Did Apperian intend for her to have access to its code and all of its data?" And Mr. Pelaggi gave the answer you knew would be the answer: "We did not, because these were sensitive, they were protected environments."

Ms. Thompson didn't get into these environments because she was given permission or because she was authorized. She got into these environments because she found a novel vulnerability, one that no one else had realized existed, and she exploited that vulnerability.

And you know who really knew that Ms. Thompson wasn't authorized to go in there? Ms. Thompson knew that herself. She had worked for AWS. She listed on her resumé -- it was her last job. One of the proficiencies she lists is IAM, Identity and Access Management. She knew how the IAM system worked, she knew what roles were, she knew they were not intended for the general public; they were intended for companies to give employees, perhaps to give machines performing processes, but to be given narrowly to people who needed those; not generally available.

And Ms. Thompson told you this time and again. This is a message she sent, a tweet between -- a direct message on Twitter between her and someone else. She said, "Then I hack into their EC2 instances, assume role their IAM instance profiles, take

over their account and corrupt SSM, deploying my back door, mirror their S3 buckets, and convert any snapshots I want to volumes, and mirror the volumes I want via storage gateway."

Ms. Thompson isn't saying that she was authorized to go in there, that this was legitimate. She's saying she hacked her way in there. And once she got in there, she says she created back doors, ways to have continued access if her other access failed.

For this message she sent to someone else, "Yeah, AWS is great, except when someone steals your IAM instance profile that has full access to the account." She's not saying she is authorized, she's saying she steals.

And you don't have to rely just on Ms. Thompson's words. You can look at her actions. This exhibit, remember, shows her computer setup. It shows how she communicated. She had her computer configured so there was a separate virtual computer inside it to communicate with the outside world, to provide additional distance so if somebody traced back, you would get to that computer, you wouldn't figure out what the main computer was. Then she went through iPredator, which is a VPN, which provides anonymity, and then she went through TOR, in many instances, another way to get anonymity. Three layers of anonymity.

You've heard a lot from defense during the trial. "Don't people use VPN for legitimate purposes?" "Don't people use TOR

for legitimate purposes?" And it's true that some people do, but that's not why Ms. Thompson was doing this. She was doing it because she wanted three layers of anonymity, because she knew what she was doing was wrong, she knew she was committing a crime.

And you don't have to take my word for it. Again, Ms. Thompson told you that. Someone else, a friend of hers who goes by the moniker "Neoice," said, "Don't go to jail, please." And what was Ms. Thompson's response, basically, don't worry. "I'm like iPredator to TOR to S3 on all this stuff." Ms. Thompson was doing this because she knew she was committing a crime, and she didn't want to get caught.

So all of this evidence, the structure of Amazon, the victims' testimony, Ms. Thompson's testimony, Ms. Thompson's words here, Ms. Thompson's actions, all tell you that Ms. Thompson was not authorized to go into those environments, she was not authorized to access those computers, and she's guilty of the charges in each of Counts 2 and 4 through 7.

Let's turn to Count 1. Count 1 charges Ms. Thompson with wire fraud, and this count charges, really, the whole scheme that we've talked about. It's the scheme to make misrepresentations to victims in order to obtain data and property, and it includes all of the victims.

And in order to prove that Ms. Thompson committed this crime, the government has to prove four things.

First, it has to prove the defendant knowingly devised and intended to devise the scheme or plan to defraud or to obtain money or property; second, that the statements made as part of the scheme were material. That is, basically, important;

Third, that the defendant acted with the intent to defraud; and fourth, that on or about March 22nd of 2019, the defendant used or caused to be used an interstate wire to carry out an essential part of the scheme.

The same evidence about what Ms. Thompson was doing proves each of these elements. First, was there a scheme or plan? Did Ms. Thompson devise a scheme or plan to defraud? And she did, because she devised a scheme to obtain money and property by trickery. Basically, her scheme was to download valuable data from companies. Sometimes she might come up empty, she might get a company where the information wasn't particularly useful, sometimes she'd hit a home run. So it was a scheme to download that property, and it was a scheme to obtain the value of computer processing for cryptojacking. And it was a scheme that based on trickery and deceit. It starts with tricking the firewall. It starts with getting the firewall to pass the message to the Instance Metadata Service, and for the Instance Metadata Service to not understand that it is an external request, and then pass that information back.

And Mike Fisk used an interesting word when he testified. He said that she was impersonating the firewall. That's really

what's happening. The Instance Metadata Service thinks it is responding to a firewall, because Ms. Thompson is impersonating the firewall, and so it provides that information.

And once she has the credentials, she uses them to gain the data, to gain access to do the cryptojacking. And in doing that, in using those credentials, she is representing that she is a person who should have those credentials, that she is a legitimate user of those credentials. She has to be a legitimate user for that to work, and so she is representing that, and that's the trickery, that's the misrepresentation.

Second, that the statements made were material, they were important, and you know they were important. If the first request to the Instance Metadata Service had said, Hi, I'm an external computer, please provide information, that wouldn't have happened -- well, first, the request wouldn't have been made. You can't communicate.

But second, the Instance Metadata Service would not have answered that. It would not provide that information to an external source.

And second, when Ms. Thompson tried to gain access to the companies' environments, if she was communicating that these credentials are being used by someone who is not a legitimate user, by someone who has stolen these credentials, companies would not provide information to that person. So these are important misrepresentations.

Third, the defendant acted with the intent to defraud; that is, did she intend to cheat or deceive these companies? And the evidence shows she did do that. She knew she was getting data that she shouldn't get and that she was getting computer resources that she shouldn't get. There's no question about that. And Ms. Thompson's own statements, again, tell you that this is the case.

Here's her first description of the data that she took from Capital One. "Jacked, this is the data that I've stolen."

Or here is another one. She said, "Whatever, I'll be employed again soon, and if I had a partner, I could have them take over my cryptojacking enterprise and be a stay at home." Ms. Thompson is acknowledging this is cryptojacking. It's stealing resources to mine cryptocurrency. She's not saying someone can take over my legitimate cryptocurrency miners. She's saying "to take over my cryptojacking."

Here is another one. A text, "I, however, hijacked more AWS accounts." Ms. Thompson knows that she's defrauding these victims.

Finally, the fourth element is, was there an interstate wire? And the interstate wire here sent on March 22nd is the command Ms. Thompson sent to AWS servers to download information from Capital One. That's the wire that's sent from Seattle to either Oregon or Virginia that begins the download of 100 million people's records. So all of the elements are satisfied

for this crime, and you should also convict Ms. Thompson of Count 1.

Count 8 charges Ms. Thompson with damaging a computer, unauthorized access to do that, and there are a number of elements -- and I'm going to come back to these in a moment and talk about how that evidence proves those elements.

But the first thing to be clear is, Ms. Thompson was engaged in cryptojacking.

Mr. Ho talked about evidence on her computer, he talked about commands used, scripts that could be used to hack those other computers, to create key pairs, to create security groups, to get access to those, to open port 22 to get access; basically, ways to gain access -- further access to computers she already hacked into and to plant cryptocurrency mining software on those. And he showed you scripts that would actually then plant that cryptocurrency software. And you've seen plans, also, where Ms. Thompson is creating new instances to use for that cryptomining.

For instance, this is a script in which she is giving -- she's, basically, assuming a role -- it's the CI/CD-Instance-Role in the top right, and it is a role that belongs to Survox, and she is assuming that role and getting its credentials, and then she's issuing commands to run instances, one after another. Those are commands to start a new virtual server, a new virtual instance for cryptomining, and she's just

starting a whole list of them.

And exactly what happens is what you'd expect happens after she does that. Survox gets a bill the next month. They usually get bills less than $10,000, and suddenly they're being billed $53,000, because there are all kinds of new instances running on their account that match the kind of instances Ms. Thompson has ordered, instances she's using for cryptojacking, using their resources.

You also heard testimony from Vincent Kenney, the computer scientist from the FBI, and he linked all this activity. He looked at the transactions that went into a wallet, wallet on Ms. Thompson's computer, and the deposits of the cryptocurrency into them. And if you remember, those started on March 10th of 2019, right as Ms. Thompson is doing her hacking, and it continued until August 5th, about a week after she was arrested.

And if you're wondering why they continued after she was arrested, it is because these machines keep running until someone finds them and shuts them down. So she was arrested on July 29th, and some of her cryptojacking activity continues to running for six days, running like zombies until they're stopped.

Those weren't the only transactions in 2019 during the period of Ms. Thompson's hacking. Witnesses were asked, well, couldn't someone else be putting money into that wallet? And if they were, why would it be during only this period? That makes

no sense. The reason they're happening during this period is because that's when Ms. Thompson has hacked into AWS, when she had access to computers to cryptojack. She's not going to do it before that, using her own electric bill and mine cryptocurrency at a loss. She's only doing it when she can do it free, from victims.

And just as with the other crimes, Ms. Thompson's own words tell you this is what she's doing. A friend asked her how she was supporting herself, and this is her response in a direct message conversation: "Just living with a friend and hacking EC2 instances and getting access to some AWS accounts and using them to mine crypto."

Or this IRC chat: "Like I've straight up gone to my counselor, told her I was hacking stuff and stealing CPU time to mine crypto, and buying new things for myself and wearing new designer clothes."

Or this text: "I have about $5,000 a month coming in now, but it's all in Ethereum, and I have to find a safe way to convert, because I'm hacking AWS accounts to get it, using EC2 GPUs miners."

So turning back to the elements, how does this prove that Ms. Thompson has committed the crime with which she is charged? Well, the government has to show these four things:

First, that the defendant knowingly transmitted a program or command to a computer, and Ms. Thompson did that. She

planted those mining scripts on each of the computers that performed cryptojacking for her.

Second, that as a result of the transmission, she intentionally impaired, without authorization, the integrity or availability of data, a program, a system, or information. And Ms. Thompson's conduct did that, creating rogue instances on computers, doing what she wants, as opposed to what the operators of those computers want. That is damaging the integrity of those systems.

It's also threatening the availability of those systems. Remember witnesses told you that if a lot of computer processing time is being used for cryptojacking, it may not be available for other things.

And you just saw a text about a client who had only 20 instances available left. If Ms. Thompson uses all those for cryptojacking, that computer isn't available to do work for the client to do their business.

And on a more granular level, and you saw the code Ms. Thompson planted, she used to do this. That code deleted logs that showed what was happening.

And these are the bottom four lines of that code. Basically, the commands to delete bash logs, commands to delete other logs, ultimately, at the bottom, the command "RM star," "remove everything."

So Ms. Thompson is destroying the logs that would show what

she's doing. And by doing that, she's certainly harming the integrity of the system.

The third thing the government has to show is the computer was used in interstate commerce. Again, computers are connected to the Internet, so that's not really an issue.

And fourth, the event caused loss to one or more persons during a one-year period of at least $5,000. And remember, Survox was billed nearly $60,000 here. Ultimately, it complained to AWS, and that money was credited back, but AWS was still out $14,000 of its own costs when it refunded that. So take out the profit of AWS's cost of running that computer, the loss it suffered was at least $14,000.

And that wasn't the only victim here. You heard evidence about other companies on which Ms. Thompson planted cryptomining, HP, PowerSquare, AT Works. And Mr. Chamberlin from AWS testified that after those were refunded, AWS lost approximately $10,000 more on those ones.

So there's no question that the loss from what Ms. Thompson did was at least $5,000, and this evidence shows the government has proved all of these elements, and Ms. Thompson is guilty of Count 8.

Count 9 charges Ms. Thompson with access device fraud; that is, attempting to possess unauthorized access devices or credit cards. And the government has to show four things on this count.

First, that Ms. Thompson knowingly possessed or attempted to possess at least 15 unauthorized access devices; second, she knew they were unauthorized; third, she acted with the intent to defraud; and fourth, her conduct affected interstate commerce.

And this count is based on Ms. Thompson's conduct after she downloads the Capital One information, what she does with it, her manipulation of that data, and the other steps she took to commit credit card fraud herself or to disseminate to others who would.

And if you look back in the evidence, what you'll see is Ms. Thompson was engaged in this course of conduct from shortly after the download, until very shortly before she was arrested. The only thing that stopped her was the government's quick action, Special Agent Martini's work in arresting her.

So let's look at that evidence.

Ms. Thompson downloaded the Capital One data on March 22nd and 23rd of 2019. Within a week, she had scanned that data or a portion of that data, and she extracted data relating to Seattle residents, and she put it together in a spreadsheet, what's been called the "Capital One inclusion list." And you have -- this is one page of it. It is a list of records for Seattle residents that includes name, address, email address, partial Social Security number.

And Ms. Thompson used this information. One of the people on this list is Joseph Baleda. Do you remember him? He's the

gentleman from Michigan, came in looking slightly bemused, and the man who liked pizza.

She pulled his record from here. She created a separate file with just his information. And we know she used it to create a Mailinator account, that's a disposable email account. You can't get records for that, so we don't know what was done with that. But the autofill on her phone had the address on that email account, so we know it was used for that.

And we know it was used for other purposes, because the autofill has Mr. Baleda's full name, address, and date of birth. So Mr. Baleda's information was put to some purpose. We don't know what, but Ms. Thompson is using this information.

She's also looking at using it for credit card fraud purposes. By early May, Ms. Thompson was doing searches on the Internet about credit card fraud. And remember those -- this is a page -- when she's looking for information about credit card numbers algorithm, how are the numbers on a credit card made so that they work, they're valid? She's looking for carding forums, that is locations where people trade information about credit card fraud, where they sell tools for credit card fraud, and they sell people's personal information for credit card fraud, and she's looking for carding forums on the dark web, in particular.

A month later, Ms. Thompson gets more practical. She is looking for servers in Russia. Remember Special Agent Henderson

from the Secret Service? He told you there is no need for a server in Russia, unless you're trying to evade law enforcement. And that's where a lot of people involved in carding keep their information.

And Ms. Thompson told you exactly why she was doing this. She told you what she was thinking by her search for server rental in Moscow.

And the next day, June 5th, she said, "My friend said something to me a while back that's got me thinking about carding a lot lately," and she refers to the algorithm, and she refers to her friend has a mag track writer and emboss kits, and said she needs those to go shopping. So you know what's in her mind as she's looking at this.

In early July, Ms. Thompson's web history shows she visited Databricks' website. Databricks is an analytic program that is used for analyzing massive amounts of information. Special Agent Henderson told you that it would be useful if you were trying to decipher the Capital One information, if you were trying to analyze that and trying to clean it up. It would not be useful unless you had a massive volume of data to work with.

In addition to looking at the Databricks website, she's also looking up a Datacard 150 embosser, a device you can use to make credit cards. It will encode them, it will raise the digits on them, it will make fraudulent credit cards.

And a couple of weeks later, in mid July, she's moving the

inclusion list, the spreadsheet that's gathered all the information on the Seattle residents, she moves it to a new location on her computer, and her web searches shows she is still looking for places to upload her data.

Now, Ms. Thompson didn't complete this plan. The reason she didn't complete it is, right as this is happening, Kat Valentine is reaching out to Capital One and alerting them to the leak, and Capital One quickly got in touch with law enforcement, and on July 27th, Special Agent Martini was assigned to the case. And it was a sensitive case. It was one he wanted to move quickly on, and that's because Paige Thompson had just posted about the Capital One information, and she said, "I want to distribute those buckets, I think, first."

And so Special Agent Martini was concerned that 100 million people's records were about to be distributed, and he moved as quickly as he could, and within a week he got a search warrant; the results of the search, you heard about the seizure of Ms. Thompson's computer and the information and Ms. Thompson's arrest.

So that plan didn't come to fruition, and the reason it didn't is because of the quick action of law enforcement.

And so if we look at the elements, the first element is the government has to prove that the defendant knowingly attempted to possess unauthorized access devices, 15 unauthorized access devices, and the evidence here shows she was working on it.

That was the goal, to either make her own devices, or to sell the information and assist other people in making devices.

Second, that she knew the devices were unauthorized. The instructions tell you that a device intended for fraud is unauthorized, and credit cards in someone else's name, there's no legitimate reason. That's intended for fraud, so that element is satisfied.

Third, the defendant acted with the intent to defraud. Same thing, there's no reason to make credit cards in other people's names, unless you're going to commit fraud.

And fourth, that the conduct affected commerce between one state or another state or between states in the United States and a foreign country. And Ms. Thompson's actions here, undoubtedly, did that. You heard from Mike Fisk and Diane Lye about the impact of the theft of that information on Capital One, how many people were suddenly working to figure out what had happened, to solve the cyber security program, to de-duplicate large numbers of records, and figure out who needed to be notified, what information had been lost.

So her actions, undoubtedly, affected interstate commerce, and that evidence shows that Ms. Thompson is guilty of Count 9.

Count 10, this is the last count, charged Ms. Thompson with aggravated identity theft, and the government has to show three things on this count.

First, that Ms. Thompson possessed, without legal

authority, someone else's means of identification. Here, she downloaded 100 million people's information. It included their names, it included other data, so there is no question about that.

Second, that she knew the means of identification belonged to a real person. Clearly, the case is she stole this information, and it was real people's records at Capital One.

And third, that she did so during and in relation to the access device fraud. And that, it's the same evidence that I've just gone through, and so Ms. Thompson is also guilty of Count 10.

So that brings us to the third thing I wanted to talk about, which is arguments the defense has made during the course of this trial.

The central defense seems to be that Ms. Thompson only accessed what the defense has called "publicly available" or "publicly accessible information." And the only thing to support that argument that you've heard was Professor Halderman's testimony.

Professor Halderman, as you remember, said, "Well, the computers functioned as they were configured, and they did what they were programmed to do," and I guess, presumably, the information is publicly available.

There's a lot of problems with that argument. The first one is the Court's instruction on what it means to act without

authority. And this -- remember, this instruction says you act without authorization when a computer is protected -- I'm going to abbreviate because I read it earlier -- but when a computer is protected by something such as a password requirement or a credential requirement, and two, the person circumvents that.

Professor Halderman's argument doesn't talk about that. It doesn't pay attention to the fact that the AWS environment is protected by credential requirements, and Ms. Thompson is circumventing those. His argument just looking at a computer and saying, "Well, it functioned as it was programmed," doesn't fit with this framework.

It also ignores everything else that you know if important. Step back from being a professor and think about the real world. Whether you're authorized or not, it matters if the company said, Hey, go into our environment or not. So it ignores what the company expressly granted authorization for and what it didn't. It ignores the length that the company went to to set up their security environment, and it ignores what Ms. Thompson knows and doesn't know. She knows she's not authorized to be in those computers. And so the fact that she found a bug, the fact that she found a vulnerability, the fact she exploited it and made the computer do something, that it did what it was programmed to, that doesn't mean that she's authorized to be in there, and everyone knows that, including Ms. Thompson.

And third, the other problem with Professor Halderman's

argument is it goes way too far. He seemed to suggest that a configuration error, that was somehow special, but it's not. It's just the same as a coding error. A coding error is an error in code written by a programmer. The programmer made a decision at each line to write that code. He might have made the wrong decision or a bad decision that leaves a vulnerability, but coding, configuration, they're all part of setting up the computer and setting up the system.

And by Professor Halderman's logic, if the computer acts as it is configured, acts as it is programmed, that's fine, and that can't be the case, because everyone who ever hacked into a computer, the computer did what it was programmed to do, that's why it let them in. And so if Professor Halderman's argument is right, there would be no such thing as computer hacking.

You were picked for this jury based on your common sense, and you should use that to look at these facts, this environment, and see what happened, and understand what happened. Follow this instruction given to you by the judge, and the evidence shows Ms. Thompson was not authorized. She was entering these computers without authorization.

I want to talk about Professor Halderman's testimony a little more.

The instructions say that you are the judges of credibility. It's your job to assess witnesses, to decide how much weight to give them. They also tell you that expert

witnesses are like everyone else. They have expertise, but it is your job to assess and evaluate the information and to use the tools that the Court has instructed you to use. And when you use those tools, think back to Professor Halderman's testimony yesterday.

Professor Halderman is the only witness in this case whose manner changed so directly between direct examination and cross-examination. He was happy to answer the questions on direct examination, but it was kind of hard for Ms. Manca to get answers to her questions on cross-examination.

Professor Halderman has taken positions before. He's written things. He was slow to agree that he had written those things, and he slowly acknowledged some of those positions. And when he did acknowledge it, he qualified them in ways that said, Oh, well, that's just the norm. That's not really -- it could be something else could be the case. He kept qualifying and changing those positions in ways that help Ms. Thompson's case.

And his memory, he had no trouble remembering a decision where a judge found that he was a credible witness, but he seemed to have a really hard time remembering details about another opinion, where a judge found that he was not a credible witness, that he was more of an advocate than an expert.

And when you look at the evidence in this case, and when you look at Professor Halderman's testimony, I want you to consider whether his testimony was more of that of an advocate

than an expert.

I want to talk for a moment also about a note, the note that was handed to someone who handed it to Eric Brandwine at a conference in May of 2019.

Now, the evidence in this case has established, basically, that we don't know who that person was. Mr. Brandwine doesn't remember who handed him the note. And so the defense is suggesting this is a disclosure by Ms. Thompson, this is her revealing this in order to help Capital One fix this, in order to fix this vulnerability.

And what I want to say to you is that the evidence in this case is clear about one thing. Ms. Thompson is not the person responsible for that note. And how do you know that? Well, first off, the note describes "own SOCKS proxy." And Ms. Thompson, obviously, is a very technologically savvy person. She came up with this exploit that no one else had thought of. She figured out how to do it. And if she were writing that note or if she were writing that note and handing it to somebody else, it would have described what happened. It wouldn't have described a different thing, something so different that when Capital One looked at it, they couldn't find the vulnerability, they went in the wrong direction. They couldn't put this together. So if Ms. Thompson were responsible for that note, it would have read differently.

But second -- and this is, actually, a really important

point -- when you look at that note, it's easy to think of it as, Oh, is this a disclosure to Capital One, and that's because this case is somewhat through the lens of Capital One. They're the ones who figured out they'd been breached and brought it to law enforcement.

But Capital One is really just a small part of this case. Ms. Thompson had dozens of victims. And you've seen some of those victims. You saw the victim Apperian, his company's entire source code and database was stolen. You've seen John Roundy, whose company lost valuable information and was subject to cryptojacking. You've seen the list of other victims.

If Ms. Thompson were making a disclosure, she wouldn't make the disclosure to Capital One. There's nothing special about Capital One. She would have disclosed to AWS, or she would have disclosed to all 30 victims.

So in hindsight when you look at this, it's easy to read it the wrong way. But what that tells you is this disclosure is not by Ms. Thompson. It might be by someone who heard her brag about Capital One, but it is not something that Ms. Thompson intended.

The defense has tried to suggest that Ms. Thompson is a white hat hacker, that she is an ethical security researcher.

Remember John Strand testified yesterday, he is the fellow from the Black Hills, which I think is North Dakota. He told you what it means to be a white hat hacker or an ethical hacker,

and he told you the norms have changed over time, but there are some fundamental things. White hat hacker is trying to make the situation better, they're trying to find vulnerabilities and fix them, and they never do certain things. They don't take victims' data. They don't cause damage to victims. They don't leak data that is not theirs. They don't engage in cryptocurrency. They don't steal companies' resources that they've hacked into for their own financial benefit.

And even if the norms are changing over time, those are things that don't change. Those are fundamental principles. And

Ms. Thompson's conduct violates every one of those principles. It places her squarely in the malicious hacker camp.

Ms. Thompson took data from companies that didn't know she was doing it. She took immense volume of data and information from those companies and she threatened to distribute them. Those are things that white hat hackers do not do.

Ms. Thompson took actions that risked other damages to the companies. She created key pairs. She created security groups. Mr. Strand told you that is incredibly dangerous. That can cause people's systems to fail. He would never do that unless he had a contract and the company said, Yes, do this as part of testing to make sure stuff is okay.

Ms. Thompson did it without worrying. And Ms. Thompson cryptojacked. She stole resources to make money for herself,

and that's as far as you can get from being a white hat hacker.

Fundamentally, Ms. Thompson's motivation was not to be a white hat hacker. It was not to help the companies into which she hacked. Nothing in the evidence suggests it was. You haven't seen anything that suggests that benign motive. What you've seen as evidence is that she wanted data, she wanted money, she wanted to brag.

And, in fact, Ms. Thompson didn't just hack herself. She talked about it with some of her friends. And this is a message that she sent to a friend. She had described -- if you go to a little earlier in the chat, she described how to download data, how to scrape S3 buckets and get data from victims, and after doing that, she tells this person, "But, yeah, if you just want to use it to learn how to do some stuff with AWS, go for it. It's not my stuff. LOL."

She's not trying to make things better. She's trying to make things worse. She's trying to teach other people how to do what she did.

Ladies and gentlemen, all of the evidence in this case shows that Ms. Thompson used her background, she used her knowledge, she used her technological savvy in order to exploit a vulnerability that she figured out. It was a complicated vulnerability. No one else had figured it out. AWS hadn't seen it, so they hadn't figured it out. No one was aware of it.

But Ms. Thompson figured it out, and when she figured it

out, she didn't report it to AWS. She didn't report it anonymously, if she was scared to. She took advantage of it to make money to support herself. She took advantage of it to take data and dig into that data and start figuring it out and start to plan to use that data for fraud. She took advantage of it to brag to friends about what she had done, and, I'd suggest, to show that she was smarter than them.

When this trial started, Mr. Klein told you you may not get Paige Thompson. But you've heard all the evidence now, and you get Paige Thompson.

We'd ask you to convict her on all of the counts on which she's charged.

Thank you.

THE COURT: Thank you, Mr. Friedman. We'll take our morning break now and do closing for the defense when we come back. So leave your instructions and your pens on your chairs, and please clear a path for the jury by staying in your seats, otherwise.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Mr. Hamoudi, you'll be about an hour?

MR. HAMOUDI: No, Your Honor. I'll be about 40 minutes.

THE COURT: And then Ms. Manca.

MS. MANCA: Yes.

THE COURT: Okay. We'll be in recess.

(Court in recess 10:46 a.m. to 11:05 a.m.)

THE COURT: Ladies and gentlemen of the jury, would you now give your attention to Mr. Hamoudi, who will give the closing argument on behalf of Paige Thompson.

DEFENDANT'S CLOSING ARGUMENT

MR. HAMOUDI: May it please the Court, counsel, Ms. Thompson.

As we said in opening, Ms. Thompson lawfully obtained all of this data. The key issue is whether she was authorized to access these computers, authorized to use computer resources, and if she was authorized, if the government cannot prove her actions are without authorization, there is no legal basis to accuse her of any of these offenses.

These were publicly known commands that the computers responded to according to predetermined rules. And because she came into lawful possession of all of this data through lawful means, there is no legal basis to accuse her of fraud, unauthorized access, access device fraud, or aggravated identity theft.

We believe the record is strong on all of these points, but any doubt on these issues must be resolved in Ms. Thompson's favor, because the government has to prove all of these elements beyond a reasonable doubt.

To understand what happened in this case, it helps to

understand a bit about Ms. Thompson.

As you heard from her friend, Mr. Carstens, Ms. Thompson has been interested in and talented with computers all her life. Due to an unstable family life and other challenges, she never completed her education, but she is intelligent and talented, especially in the area of computers. She's had jobs in tech fields, but her work is intermittent and not stable.

As true of many who love computers, Ms. Thompson spends a great deal of time in a virtual world. She often is up late at night, typing code and talking to people who share this world with her, constantly exploring what is possible in this online world.

Computers provided her with access to a community, but there also have been times when she's felt isolated and alone. In those times, as you heard her longtime friend, Tim, state, she's known to say troubling things that she doesn't truly mean in order to get attention, to get a response.

The government has admitted an overwhelming amount of computer evidence and social media evidence to try to make what happened here seem alarming and frightening. But as Mr. Halderman testified, what Ms. Thompson did was quite simple. Any member of the public, with these rudimentary skills, could have done the same.

My presentation today will cover what technically happened, how Ms. Thompson behaved after she freaked out, learning what

she found, what the companies and the government did in response when they learned, and how we find ourselves here today.

When I refer to the jury instructions, please, if you can, note them for your deliberations.

What technically happened demonstrates that Ms. Thompson's access was authorized, and demonstrates that there was no fraud. By both technical and legal definitions, the computers Ms. Thompson accessed were open to the public, meaning her access was authorized.

You heard testimony from Ms. Lye, who reviewed the memorandum to the chief information officer at Capital One, Rob Alexander, and in that memorandum, she stated she was aware that the web application firewall had been granted overly permissive access, and Ms. Thompson was able to "access our AWS storage from outside the Capital One network."

And Mr. Fisk, from Capital One, after cross-examination, effectively conceded the same thing. Here, if you look at what they themselves have conceded, they admit that Ms. Thompson's access to these computers were authorized.

Now, the government points out to you, during their closing, that really it's the company's intent that matters. Mr. Fisk's intent, Mr. Chan's intent, Apperian's intent, Mr. Pelaggi, or any member of these companies, it's their intent that matters.

But that's not what the law says. The law says "the

computer." It doesn't focus on an individual representative's intent within the company or the policies set within that company.

Why is the law written this way? Why is the law focused on the computer and not on the person? Because people could be sued or charged with a crime simply because of the computer's configuration.

You heard testimony from Professor Halderman that these are real risks. You've heard testimony from their own witness, Mr. Strand, that these are real risks, and for that reason, the law focuses on the computer. It does not focus on a person's subjective intent.

The testimony offered by Ms. Lye about the company's understanding of this configuration that was corroborated by Mr. Fisk was really expanded upon by Professor Halderman in his demonstrative.

He laid out what really happened here. He said that Ms. Thompson wrote a simple command, a scanning command, which reached out to the proxy and said please ask the Instance Metadata Service for available credentials. The EC2 instance ran open forward proxies. This was a decision, by someone inside Capital One, to configure the computer this way. That rule allowed anyone to use, to make requests to other servers, including the Instance Metadata Service, and the response was "okay."

The next event was that the Instance Metadata Service, please, send me available credentials, and per its rules, it provided role credentials in response to requests from the EC2 instances. "Okay."

And the next request, here's a credential, please send me data, launch, and instance. Capital One configured -- all of these companies configured their computers to allow some or all of these events, allow anyone -- Capital One -- possessing role credentials to read data, launch EC2 instances, or perform other actions for which the role has been granted permission. That's exactly what happened here.

And it is important to understand that Professor Halderman's technical opinions went unchallenged.

Instruction 18 to 23, which deal with Counts 2 through 7, all require the government to prove without authorization beyond a reasonable doubt.

Professor Halderman's testimony, Mr. Fisk's testimony establish that Ms. Thompson's access to Capital One's computers were authorized.

Witness after witness testified that this system was overly permissive. Overly permissive does not mean without authorization. It is exactly the opposite; too much authorization.

Professor Halderman's conclusions, again, the technical opinions went unchallenged. Here, all of the companies

configured their firewalls, the web application firewall granting overly permissive access to Ms. Thompson, who was able to access the systems for all of these companies from outside their network. Ms. Thompson had no say over the decisions of these configurations.

Now, the companies all had different types of data stored in these S3 buckets.

Capital One had 1.7 terabytes of data, some of which was sensitive.

Apperian, 700,000 file paths, and inside of them were databases that are of great value to them.

Bitglass, internal log files, which, I believe, Mr. Chan testified were not worth anything.

42Lines, instance information.

Enghouse, survey results.

We called two additional entities. Ohio State said it was public data; Michigan State, public data.

The government has made much of the companies' intent here, but, again, their intent is irrelevant. The concept of "without authorization" does not focus on the company's subjective intent, and the proof here, the only proof here that matters is how the computers were configured at the time of access.

Instruction 17, which deals with wire fraud, requires the government to prove beyond a reasonable doubt that there was a misrepresentation of a material fact, and that Ms. Thompson had

the specific intent to deceive and cheat these companies out of money or property.

Professor Halderman's testimony that the system operated exactly as it was designed demonstrates that there was no such misrepresentation, there was no trick. Ms. Thompson used publicly known commands recognized and authorized by AWS computers, because that is how the companies configured them to run the commands. The computers were not tricked. They executed commands as they were configured and programmed to do.

The testimony and data demonstrate that Ms. Thompson had no idea what sort of data she did find as she was downloading it. There was no specific intent to deceive and cheat any particular company. And, indeed, there is evidence that once she discovered what she had accessed in Capital One's S3 buckets, she attempted, in some form or fashion, to notify Capital One about the vulnerability.

Let's be clear: In the approximate five months Ms. Thompson possessed Capital One's data, she never shared it, she never made credit cards, she never opened bank accounts, she never took any efforts to sell it. The same is true as to all of the companies here.

There 's strong evidence of her lack of intent.

Mr. Schuster, from AWS, provided favorable testimony to our defense. He spoke about how the business model -- briefly, when the Court inquired -- was about taking things off from physical

premises and into a shared space. That is the concept, the shared space. Obviously, government and the defense disagree. But if you carefully listen to his testimony, there are many areas in which the witnesses do agree, as Mr. Schuster testified. Capital One set the rules for its firewall and chose to allow external requests. Capital One enabled their proxy to allow a forward proxy to reach its Instance Metadata Service. Professor Halderman's opinion on this point went unchallenged.

The credentials provided to Ms. Thompson allowed access to some S3 buckets but did not allow access to others. Some gates were up, and some gates were down, which signaled that some access was authorized. Again, this was based on the decisions, choices made by Capital One and the other companies that determined whether she could or could not do that, based on her program-based requests.

Mr. Schuster, from Capital One, said that Ms. Thompson tricked the firewall. There was no trick. As Professor Halderman testified, by default, there were no permissions for these roles. In other words, it was a conscious, affirmative action to set up these roles. If there was a trick, then someone would have testified that the software was patched afterwards, so it couldn't be tricked. There was no patch, because, as Professor Halderman's experiment showed here in court, the software operates in the same way today.

Ms. Thompson's ability to access the data was a direct

consequence of Capital One and the other companies' decisions to set up their software and access provisions.

In fact, on cross-examination, Mr. Schuster admitted that companies would intentionally configure their proxies in this way.

What's novel here is the government's theory about what constitutes hacking. The government is trying to portray a narrative that the Identity Access Management Role credentials are like an ATM, a PIN, a password. They're not. They're automatically assigned by AWS's system to do what the web access firewall is confirmed by the client to do.

The government said that this was novel, no one knew, but that's not true. Professor Halderman told you that the settings of the web access firewall to operate as an open forward proxy was in Apache's documentation.

Ms. Thompson is here because she read the instruction manual, and Capital One did not.

Mr. Fisk, from Capital One, provided favorable testimony to our defense. Mr. Fisk testified that Capital One's firewall allowed a command line, which was reasonably straightforward, for Capital One to reproduce to allow requests from Capital One to go through the firewall and be proxied to the Instance Metadata Service.

That testimony means that the computer was not protected by generally applicable rules regarding access permissions. That

testimony means that Ms. Thompson did not circumvent the rule regarding access permission to gain access to the Instance Metadata Service. Their computer allowed it. This is exactly what Professor Halderman explained, in great deal, and his explanation went uncontested by the government.

Remember that the government did not take issue with that. The government did accuse Professor Halderman of overly simplifying.

Professor Halderman's slides were made to explain some of the concepts to which he testified to in accessible ways. He testified to much more detail as he presented these slides, including that the proxy scanning here was quite simple and could have been accomplished by a web browser, manually, albeit at a much slower rate.

If you recall, on cross-examination, Mr. Fisk admitted that. He admitted that you could use a web browser to send a request to this web access firewall, just as they had to admit that using TOR, iPredator is okay to use, because he said, "We can't disable it because we may exclude some of our customers."

Mr. Fisk, from Capital One, testified that the data was copied from their S3 buckets, on March 22nd, 2019, by iPredator and TOR. Everyone admitted, again, that it's legal to use these services. Mr. Fisk testified -- well, this is an important date.

Under Instruction 17, Count 1, wire fraud, this is the

wire. This is the wire. It is the wire that serves as the basis for the accusation under that count.

There is no evidence that Capital One was cryptomined, none. Mr. Fisk never testified to it. The request on this date granted access to the server. What this means for that count is that there was no misrepresentation of material fact. He admitted, on cross-examination, that Ms. Thompson would have no idea what the content of the data was that she was downloading. That admission is important, because it means she has no intent to deceive and cheat the company of money or property, because she does not know the content of what she is downloading. She did not visit that S3 bucket knowing beforehand that Capital One would have buried, in 1.7 terabytes of data, sensitive information.

Ms. Lye, from Capital One, testified that it took hours for her team to go through that puzzle to determine what that data was.

Mr. Fisk testified that a cyber security professional from Capital One learned that external request was made to Capital One through iPredator, but did not identify anything wrong with it. The reason this professional did not is because the access looked like normal activity, meaning the system operated as it was set up.

This event is important for Instruction No. 18, Count 2, because it demonstrates that between March 12th, 2019, and July

17th, 2019, Ms. Thompson's access was authorized.

On cross-examination, Mr. Fisk admitted that Ms. Thompson was effectively authorized to access their servers and download their data.

Initially he said, on direct examination -- or I believe it was cross -- that she stole credentials, stealing credentials. She's not charged with theft. She's charged with unauthorized access. And that is why, when I put his own testimony that he gave under oath in a prior proceeding and asked him to answer the question asked in that proceeding, he said -- he testified under oath that she was provided credentials and provided access to data. And he admitted, following that, that those credentials would be obtained from a public web browser.

That evidence is critically important, because not only does it establish that her access was with authorization, but it also establishes, under Instruction 17, Count 1, that this is no false representation of a material fact.

The April notification. Mr. Fisk testified, in April of 2019, another Capital One cyber security professional was notified that the system had granted credentials to an external user. The analyst closed out that notification as well.

Professor Halderman agreed, with evidence that he viewed, that this was a loud and proud scan to trigger Capital One's alarms.

Intended to notify, technically. The reason why this is

happening is that Capital One's configurations were overly permissive.

Again, under Instruction 18, Count 2, Ms. Thompson's access on this occasion was authorized.

Under Instruction 17, Count 1, this was an intent to notify, not an intent to deceive and cheat Capital One out of property or money. This evidence is, again, also important, because not only does it establish that her access is with authorization, but it also establishes that there was no false representation of a material fact.

The May notification. In May of 2019, AWS and Capital One received a note that you have seen and heard testimony about. Professor Halderman testified that this note referred to the same vulnerability involved in this case. He opined that Capital One should have been able to identify the vulnerability through this note.

Capital One was notified, time and time again, about this configuration issue by AWS's program GuardDuty, by the multiple scans Ms. Thompson conducted, by the note passed to AWS. Capital One failed to handle the issue. How do we know that? We know that because federal regulators found as such when they imposed an $80 million penalty.

As Professor Halderman said, Capital One, potentially, did not want to make this data public, but they did. That choice, however inartful, signaled to Ms. Thompson that the data she

accessed and copied was public and authorized.

The note does not say "steal credentials." It says it can "hit credentials," which means it can reach credentials through a publicly facing IP address.

Mr. Brandwine admitted that they could determine who the account belonged to from that IP address. He admitted that that person who handed him the note stated that he was asked to pass the note to him.

And Exhibit 1013, Robert McLean wrote multiple security professionals on August 2nd, 2019, saying that, "We are confident," "We assess this was either Thompson or her associate Neoice." This is the confidence of cyber security professionals expressed in an email. This email, coupled with Mr. Brandwine's testimony, along with the authorized accesses in March and April, demonstrated that Ms. Thompson was disclosing the vulnerability.

Ms. Valentine, who does not work for Capital One or Amazon, who saw the gist that the IP address -- when she testified, she said the IP address screamed out at her when she looked at this note.

The company's attempt to suggest to you that the note does not place them on notice is simply not credible. You are free to consider -- free to consider -- whether the failure to take this note seriously was one of the reasons regulators imposed the fine on Capital One.

Under Instruction 17, Count 1, this note is an intent to notify, not intent to deceive and cheat the bank out of money or property.

Under Instruction 25, this note was an intent to notify, not an intent or an attempted intent to possess unauthorized access devices with the intent to defraud.

May 26th. Mr. Fisk admitted, on cross-examination, that the attempted access on May 26th, which took place after the note was passed, was an attempt to see if the access still existed.

Look at the CloudTrail logs that were admitted showing all the access to Capital One's system. Look at the similarities in the IP addresses. Again, Instruction 18, Count 2, the computer authorized her access. This evidence is, again, also important, because not only does it establish that her access was with authorization, but it also establishes, under Instruction 17, Count 1, that there was no false representation of material fact to gain access to the server.

Now that I'm finished talking about what technically happened and have discussed the note, I want to discuss what happened next, and its evidentiary significance.

Ms. Thompson's disclosure to Ms. Valentine demonstrates that she lacked any intent to commit fraud, access device fraud, or aggravated identity theft.

It was a disclosure, messy and, perhaps, inartful, or

ham-fisting about a serious vulnerability that no one was taking seriously.

Tim Carstens testified that her words and online statements have made it hard for her to be taken seriously. He testified that her comments are not always appreciated outside the friend online community.

By way of background, fear may have also played a part. Ms. Valentine, Mr. Strand, Professor Halderman all agree that disclosure is difficult. Professor Halderman testified that he has been threatened with lawsuits and that associates have been arrested. He said it is daunting. Mr. Strand testified that people can be sued.

There is a power dynamic in this world of cyber security, and you've heard evidence of it that explains the difficulty surrounding disclosure.

Ms. Thompson is a transgender woman in a community that can be, as Ms. Valentine testified to, a toxic and hateful culture. She does not have a high school degree or a college diploma. She does not have a large company or academic institution behind her. She has little power in a world set up not to believe her.

So Ms. Thompson reached out to Ms. Valentine, a woman who identified herself, publicly, as a hacker, who previously worked in credit-card compliance in June 2019. Her disclosure was erratic and provided Ms. Valentine a private link on a gist, which allows people to provide their notes, and, here, she

received the proof of consent that showed that Capital One had set up its AWS in a manner that allowed public access to it. Ms. Valentine initially described the message as outlandish, which corroborates exactly the testimony of Mr. Carstens, who said Ms. Thompson was not taken seriously by people. The messages forced her to block Ms. Thompson. Mr. Carstens said she would spam a lot of comments on message boards when she communicated.

Even Ms. Valentine, a person who is well respected in the cyber security community, talked about her own fear of disclosure, even though she had law enforcement ties. She had a professional disagreement with a colleague as to whether she should disclose. Ultimately, it was the fact that Ms. Thompson threatened to dox people's identities is what drove her to disclose.

It is important to understand that the term "doxing" is a terms of art. Professor Halderman testified that it means going public. Ms. Valentine's interpretation of that term should be considered in light of the fact that she did not know anything about the note and the prior attempts to notify Capital One's systems.

Mr. Carstens, who testified as to her reputation, said that she makes statements to grab people 's attention. There is sufficient evidence on this record for you to conclude that Ms. Thompson was going to go public because she was not being

taken seriously, because, in her life, she struggled to communicate.

This is why Ms. Valentine instinctually, ultimately, interpreted her message as a cry for help. We contend it should not be interpreted to mean that she truly intended to dump Social Security on the Internet. She has had this data since March and did not do that. And she said this to Ms. Valentine; she did not do it and it remained in her possession for another month. She was trying to get attention in an erratic way.

The facts that I've just described to you as to Ms. Valentine demonstrate that Ms. Thompson did not have an intent to deceive and cheat under Count 1, Instruction 17; under Count 9, Instruction 25; and no attempt to commit aggravated identity theft under Count 10, Instruction 26, because she told somebody in cyber security about this.

So why are we here? Power dynamics. We talked about that in opening.

Capital One has a strong interest in projecting an image to the public that they take their data security seriously. That projection impacts the financial viability of these companies, their share prices, and their bottom line. They have a clear interest to limit liability. They have a clear bias in deflecting blame away from themselves to someone else, anyone else.

That interest was made clear to you. On direct

examination, Mr. Fisk incorrectly suggested to you that the fine imposed by government regulators did not involve this breach, saying it was a broad consent order. In their annual report, they told the public that the $80 million penalty was tied to this incident, but he suggested to you, under oath, that it was not. And if you look at the consent order and read it together with the 2020 annual report, the evidence shows this:

Ms. Thompson's access to these servers led to a stark revelation that the bank had failed to protect their customers' sensitive data since 2015.

As you recall, Ms. Lye testified that she was aware that her supervisor, Mr. Rob Alexander, chief information officer, informed the risk committee in a memo, a group of senior executives at Capital One, that this breach occurred because the web access firewall had been granted overly permissive access, and Ms. Thompson was able to access their AWS storages from outside the Capital One network. I asked her that. She said she was aware. This is exactly what Professor Halderman testified to. That evidence and testimony by Ms. Lye demonstrate no intent to defraud, no aggravated identity theft, no access device fraud.

In the 2020 annual report, they defined the cyber security incident to shareholders as, quote, the unauthorized access by an outside individual who obtained certain types of information relating to people for our credit card products and to our

credit card customers that we announced on July 29, 2019.

No mention of what Mr. Alexander wrote to the risk committee. Capital One effectively convicted her in their annual report.

But if you look at the law as instructed by Judge Lasnik, instructs you "without authorization," her access was authorized.

Again, Ms. Thompson never monetized this data, never disseminated it, never made any use of the data to financially benefit herself or harm Capital One's customers.

What Ms. Thompson's sin is -- what Ms. Thompson's sin is, is it appears to be that she spoke about what she did in an ineloquent, facetious, offensive, and arrogant way. That does not make you a criminal. A person's statements, even erratic statements suggesting criminality, do not make you a criminal.

Look at Instruction 13. You decide how much weight to give to any particular statement, including the circumstances under which they are made.

You heard no evidence from anyone at the other end of Ms. Thompson's statements. Actions speak louder than words, and Ms. Thompson's actions here, or her lack of actions with the data, are the evidence of intent you should rely on.

So after Capital One learns that the data is breached, the FBI is contacted by Capital One, and they acted very quickly. But those actions were only informed by Ms. Thompson's tweets.

None of the background about the prior notifications were known to the FBI at the time. These are the March-April notification that were ignored by the cyber security professional at Capital One, the May 20 note, and the access subsequent to sending that note to see if the data was still publicly available, the scan triggered the alarm.

Capital One never really allowed its corporate executives to meet with the FBI directly. Most or all communications were through lawyers. Capital One had their representative seek information directly from Agent Martini to provide it to the OCC, because they knew they had liability. This is before the fine is imposed. That same person who was seeking that information from the OCC, whether it was a joke or not, offered to buy Agent Martini a drink. But Capital One doesn't tell Agent Martini about the note. Those are the power dynamics. In fact, it is unclear if they ever told Agent Martini that multiple cyber security professionals inside Capital One had confidence that Ms. Thompson or her associate were the source of the note. If that was the case, he would have testified to it.

Ladies and gentlemen, this evidence is significant for you to understand that Ms. Thompson is defending herself on multiple fronts. She's just not defending herself against the government, but also against corporations with significant interest in the outcome of this case. All of these companies have a vested interest in projecting an image that they take

data security seriously, power dynamics. Why? The law is very uncertain in this area. That's why. It is unclear who is responsible.

I want to talk about the front door. Let's talk about the day of the search warrant.

It's 6:00 a.m., and the FBI shows up at Ms. Thompson's house with 30 to 40 agents dressed in fatigues and armed with assault rifles and a battering ram. Agent Martini would not directly admit that she is a physically slight woman. You can conclude whether she is or not, based on your observation of her throughout this trial.

They disabled the security camera at her house and proceeded to raid her house. There's no evidence of how much sleep she got or how scared she was. Ms. Thompson provided the government with all of her passwords, which she didn't have to, but the government focused on the fact that some of her statements were not entirely truthful. Again, look at Instruction 13. Look at the circumstances, and evaluate the statements in the context in which they were given. Imagine how scared and nervous you would be if that many armed individuals raided your house.

We were deprived of the opportunity to present to you the circumstances surrounding the statements she made on that morning, because the video was destroyed for tactical reasons.

What did they find after the raid? They found data. They

found nothing that she shared the data or monetized it. Over the last three years, they have had access to her social media, phones, emails, public postings, servers, server archives, and on and on and on and on, but no evidence that she misused anyone's data.

Remember the government told you there would be evidence of designer clothes? The evidence showed no designer clothes.

We also learned that all these companies -- Apperian, Bitglass, Survox, 42Lines -- all had provided overly permissive access to their servers, like Capital One. Professor Halderman explained why, in his demonstration, all of these companies' firewalls were configured the same way. That is significant under Instructions 19 through 22, which represent Counts 4 through 7. Ms. Thompson's access to their servers was also authorized.

Count 8. Count 8, remember when I talked to you earlier about why, under Count 1, there was no false representation of a material fact to gain access to a server? And remember when I said there was no intent to deceive and cheat the companies of property? All of those arguments apply to Count 8.

Here, the government cannot prove, beyond a reasonable doubt, that Ms. Thompson transmitted code to a computer between March 10th to August 5th, 2019, which intentionally impaired, without authorization, the integrity or availability of data.

Why? Mr. Schuster never testified that Ms. Thompson did

that. He's one of the highest representatives from AWS.

The mining script identified by Mr. Ho was never executed or tested by him on a device to see if it actually impaired a computer.

Professor Halderman testified that creating a new instance, which is what you have to do to mine cryptocurrency, does not impair a computer, because what you're actually doing is just creating a new computer.

No testimony was received from representatives from Capital One, Survox, Apperian, Bitglass, or 42Lines that their computers were impaired.

But most importantly, this instruction also requires the government to prove, beyond a reasonable doubt, that this access was unauthorized. If the computers permitted somebody to create new instances, this is an authorized act.

And, factually, there was no evidence tying the wallet that was on Ms. Thompson's computer to Ms. Thompson, other than some web searches.

Agent Ho found keys on the computer, but no one tied those keys to that wallet.

Mr. Chamberlin, who came here from AWS, testified about billing. He never talked to any of the customers. He never bothered to see if they had other accounts that would account for these anomalies. He didn't investigate thoroughly to level an accusation against my client. He just looked at some bills

and said he's drawing an inference.

Agent Ho received abuse reports from AWS, and he testified that those abuse reports did not specify cryptomining. If the mining was a priority to the government, they would have had Agent Kenney and Mr. Chamberlin involved much earlier. It was not. Because they saw how she was living when they went into her house to arrest her. The manner in which she lived did not reflect the statements that she was making: "$5,000 a month," "designer clothes," "BMW," "my stocks." Read those statements.

Count 9 and 10, aggravated identity theft and access device fraud. The government introduced evidence that, roughly, 100 million people's data was taken. Ms. Lye testified that 117 people's data was kept in text files by Capital One, and yet the government had a single person alleged victim, Mr. Baleda, a person who testified that he never suffered any negative consequences, not even a credit hit, from this data leak, and yet Ms. Thompson has been charged with attempted access device fraud and aggravated identity theft.

The following acts, as to Mr. Baleda, do not amount to a substantial step as defined under Instruction 24. Looking on the Internet for 20 minutes, having his information on your phone and creating lists all on different dates does not unequivocally demonstrate that access device fraud would be committed. She did not commit aggravated identity theft.

Agent Henderson, on cross-examination, admitted that if you

took his Internet searches and cobbled them together over a long period of time, selectively, you could make suggestions about him.

Before I sit down, I want to say that I won't be able to get back up after the government offers their rebuttal, even though I want to.

When the government starts talking about statements, social media postings and such, I want you to imagine someone takes your text messages, emails, social media statements, Twitter, Facebook, whatever, over a long period of time, months, and imagine the government and the FBI get these materials, and they, through their investigatory, accusatory, and suspicious lens, select random messages from each of these platforms, cobble them together, and try to paint a vignette about who you are.

It has been an honor representing Ms. Thompson. Her Netcrave Slack channel is called "Never Give Up on Your Dreams." No one should ever give up on their dreams.

You heard about Ms. Thompson from Mr. Carstens. At 14, she was known as Zero, she talked about programming, she was very capable, she was part of a smart group where others have advanced, and she was up there in the group in terms of her abilities. Then her handle changed to "Erratic." It was not self-imposed. It was a reflection of how she was viewed by her friends, because she would spam a lot, a lot of comments, very

erratic.

What led to this may be a mystery to you. When Mr. Carstens talked about not feeling comfortable when he went to pick her up at her house, I wondered what life was like in that home. I truly wonder if that home provided the support that one would need to thrive, like the many computer professionals who testified in this court, having graduated from esteemed universities; this is another reason we ask that you pay attention to power dynamics.

When you look at her statements, remember what Mr. Carstens said. What that means, I think, is that you have to know someone before you judge them by their words. All we can do, as outsiders, is judge them by their actions. What she did here is lawful.

I do want to finally speak to you about one last aspect, which is the idea of reasonable doubt. This is Instructions 2, 3, 4, and 27.

When I talk to my students about reasonable doubt, it's a hard thing to talk about. It's a hard thing to teach. It is a hard thing to explain. I request that you approach the task of reasonable doubt with a willingness to speak the hardest words in life to utter, "I do not know." When we say that, "I do not know," we are, at times, apt to feel like it means we have failed or we are not living up to that task. The words "I do not know" might even mean we're confessing, for a moment, that

life does not make sense.

But when you go into that jury room, be gripped with courage to speak those words if you determine them to be appropriate. That is what a not guilty verdict means. It means, in plain terms, we do not know, not for sure. Not guilty does not mean innocence, not necessarily. It means something a bit different. If you say not guilty, you're saying as a group, "we have thought hard about these charges and this evidence, and we do not know for sure." That may be the wrong answer in different tasks, in occasions of your life, but not in the jury room. Do not feel that you have failed because you come to that conclusion. In fact, it is your solemn obligation to say those words if they are true.

You must convict only if you are convinced the government has proven all of these elements beyond a reasonable doubt. But if doubt remains -- and, frankly, it clearly, clearly exists in this case -- if you find reason to doubt, then come back here, stand before us all, and say in substance, "We don't know for sure."

In this life we know many things beyond a reasonable doubt; that we love our children and express that love in a way that allows them to thrive and to realize their greatest potential. But that love means we will tell them, through words and actions, to never give up on their dreams.

Ms. Thompson did not commit any crimes. For the government

to say otherwise, do you know that? Do you know for certain? Do you know for sure? Even if you have doubt between weighing the testimony of Agent Ho, Professor Halderman, Mr. Fisk, Mr. Schuster, that doubt must get resolved in Ms. Thompson's favor. That's reasonable doubt. Return a verdict of not guilty on all of those counts. Bring this nightmare to an end for her.

THE COURT: Thank you, Mr. Hamoudi.

So because the government has the burden of proof, they get the last word in closing argument. So the only thing between you and lunch and deliberations on the case is Assistant United States Attorney Jessica Manca, who will make the rebuttal argument on behalf of the government.

GOVERNMENT'S REBUTTAL ARGUMENT

MS. MANCA: That's Judge Lasnik's way of telling me to be brief, right? And I will be brief, because you've been here all morning listening to the evidence.

You've heard a lot of technical evidence, and Judge Lasnik described it as sort of learning a different language, and the law can be like that, too, like learning a different language.

But something to remember when you go back into the jury room is, we don't use computers to decide the guilt of a person. We don't feed data into programs, and then spit something out to make a decision about whether someone is guilty or not.

What we do in our system of law is we ask jurors, like yourselves, to bring your common experience, your lived

experience, into the interpretation of law.

And what Judge Lasnik told you is that there are terms defined in the jury instructions, and those terms provide the contours, the framework for your analysis, but you will find words in the jury instructions that are not defined for you, and you use what Judge Lasnik referred to as the common meaning of those terms. You are the interpreters of those words, and what you do is you take your lived experiences and your common sense, and bring them to those instructions.

And it's helpful, when you're in the jury room, to think about the reason behind the law. Why does this law exist? Why does this term exist? What is it trying to prevent? What is it trying to allow? And that helps frame the discussion.

An example of that is authorization. What is the law trying to do? There's tension between security, you know, people who are finding vulnerabilities, and the companies who are trying to keep the vulnerabilities out.

And the law says, what should a person do when they find a vulnerability, right? And the law is acting on that moment, that decision-making of "I found a vulnerability, what do I do next?"

You can imagine a case where a company would make such a huge technological mistake, that it actually exposes private information to the general public, like accidentally posting Social Security numbers on the Internet. That is not this case.

This case involved a complicated series of steps in which Ms. Thompson circumvented the security systems that keep most people out, security systems that involved usernames, passwords, credentials, multifactor authentication.

So don't buy into this hypertechnical argument that a machine executing commands by itself is authorization.

If someone hacks into a bank account and issues a command to withdraw money, the system will work as it's intended to do. It will withdraw that money, but that won't be authorized.

If you even go lower tech for a moment, let's say a person puts their house key under a doormat, right, their spare key, and someone comes along and starts looking under all the doormats on a block, and finds a key and uses it to unlock a back door, when a key fits into the lock and it unlocks the door, the key is doing what it's supposed do, it's unlocking the door in response to the key. That doesn't make the person's entry into the house authorized.

The defense is trying to convince you that it doesn't matter that these companies didn't want their data downloaded, that it didn't matter that they tried to protect it, that it didn't matter that they didn't want these credentials to be used this way, and they didn't know that their web facing applications were talking to an internal resource. Guess what? It does matter. It matters a lot.

And Dr. Halderman's testimony ignored several critical

steps in the hack, which I'm going to talk about in a moment. But there's something much more significant missing from his analysis. It's the human component of these systems.

We don't live in a world where machines are just off doing things on their own. Computer systems are built and configured and operated by people, and people make mistakes. It is inevitable, and computer security flaws are inevitable. That's why Eric Brandwine, you know, distinguished engineer, said the goal of security is not to eliminate vulnerabilities; it is to understand and mitigate risk.

But the defense is suggesting that if any computer system anywhere has a flaw, it's open season, right? A person can access the systems and do everything they want, as long as the computer keeps responding to commands. That's not the law, right? Your instructions tell you that's not the law.

Circumventing security systems is a crime. And what it means to circumvent a system is to use applications and credentials in a way they aren't supposed to be used. That's why it matters that the web application firewall wasn't supposed to be grabbing credentials from the Instance Metadata Service. It's a traffic cop. It's just supposed to be a traffic cop.

And that's what it means for these technological components to be overly permissive. The defense kept using the words "overly permissive." It means that it just had more powers than it needed to have. It doesn't mean that Ms. Thompson had

permission to use those powers.

Circumventing a system is also accessing data in a way it's not supposed to be accessed. Take Bitglass as an example. To access Bitglass's data, Chris Chan testified that employees needed VPN access, which requires account authorization and multifactor authentication, and a jump box with an SSH key and two-factor authentication.

Survox is another great example. When an employee wants an IAM Role, that employee sends a request to John Roundy, who evaluates whether the employee needs that role, and then there is a multifactor authentication token. It's simply not true that these IAM Roles are supposed to be generally available to the public.

And attaining credentials from the Instance Metadata Services to grab cold storage data from Survox's S3 bucket is circumventing the system that he and his company have set up to control access to their private information.

And one of the ways you know that Ms. Thompson used a back door to access this data is that when you look at the data in the jury room, it looks like it was vacuumed out of a back door. Right? It's the back-end data for a database.

And, of course, stealing credentials is circumventing security features.

There is a second human component here, which is the people trying to break into the systems. What is their motivation and

intent? Is it to make the company better or stronger, or is it to take something from them? Is the person hacking for other people, or are they hacking for themselves?

It matters that Ms. Thompson knew what she was doing was wrong; that she was, in her own words, stealing credentials, stealing data, and stealing computing power. It matters a lot. And the best evidence of her intent is what she said and what she did at the time of the crime.

Because as between the company that doesn't know it has a security flaw, that tried to set up the security systems, but through misconfiguration has an unintended consequence, as between that company that doesn't know it's vulnerable, and Ms. Thompson, who knows the company is vulnerable, who is in the position to stop the breach? She is. She is in the best position to stop the breach, and she chooses not to, and it's that choice that is crossing the line.

I want to just say a few things about the note. It's Exhibit 1013, which you'll see -- I'm sorry. 1013 is the email from Capital One. Just look at that, because the note says, "We are confident in this discovery regarding the conference," it's the wrong date, it's the wrong conference, it's the wrong city. They're wrong about literally everything. People can be confident and wrong.

The same thing with the loud and proud scan. What does that even mean? There's no evidence of that.

And if Ms. Thompson wanted to disclose this information, why is she still searching for servers and embossers and carding forums on the dark web? She is Googling all these things. You know what she's not Googling? "Responsible disclosure Capital One," "how to report security vulnerabilities to companies."

Ms. Thompson had no legal obligation to do a responsible disclosure. But the fact that she has that off-ramp available to her and chooses not to take it is evidence of her intentionality and awareness that her actions are unauthorized.

So if we could show Exhibit 117. This is the script to scan -- this is the first step. It's scanning IP addresses and grabbing that metadata, looking for that IAM ID.

Put up Exhibit 643, page 5.

This is a list of vulnerable IP addresses. These are the internal servers that she is able to reach through this proxy. She could have taken this to Amazon for responsible disclosure, but she doesn't. What does she do?

There's Exhibit 119.

Grabbing the name of the IAM Role, and then what does she do?

Exhibit 609.

All the IAM names. And she doesn't stop there, either. She doesn't take this list of IAM Roles to Amazon. What does she do?

Exhibit 120.

She takes these IAM Roles to the company's Amazon command line interface, and authenticates into the company's account.

Can we do Exhibit 670, page 2?

There's a lot of technical evidence in this case.

Can you highlight "hashtag get security credentials"? Thank you.

We put an FBI computer scientist on the stand for five hours to explain the evidence on Ms. Thompson's giant computer, and we did that for two reasons: Number one, you need to see the facts, and number two, we bear the burden of proof beyond a reasonable doubt, and we take that burden of proof very seriously.

But at the end of the day, this case really is as simple as "hashtag get security credentials." Because wherever the line is that divides authorized access from unauthorized access, "hashtag get security credentials" is on the unauthorized side of that line.

So if you saw this script and thought to yourself, "this cannot possibly be legal," you're right, it's not.

Can we do Exhibit 120 again?

So she uses the role to authenticate into the IAM account, and does she even stop there? No, she does not. She lists budgets. She describes instances. She creates security groups. She creates key pairs. And does she stop there? No, she does not.

Can we have Exhibit 204, page 47, and can you highlight that last comment?

She lists the buckets, and then she downloads the data. And what you'll notice about this Exhibit 204 is that this is a comment to her gist. So she had the information she needed about listing the buckets, and then takes the additional step of syncing the information, and then she posts it on GitHub to say, look, I downloaded that data.

And then there is Exhibit 122, which is cryptojacking. And in order to cryptojack, she has to create a new instance, she has to open port 22 using security groups -- that's that connection to the EC2 instance -- she has to create a key pair to connect through this back door, and she has to create a Secure Shell connection.

By the time she gets here to installing the mining program, there are at least eight off-ramps that I just described to you that she chose not to take. And the availability of those off-ramps and her choice not to take them gives you tremendous insight into her intent. She is missing these off-ramps one after the other, because her true destination on this highway is taking data and cryptojacking.

It is not at all unclear what the law is or what happened here. You are sure. You know what happened. Ms. Thompson had a large-scale hacking scheme. She hacked into these companies without authorization. She stole credentials. She stole data.

She stole computing power. She is guilty of these crimes beyond a reasonable doubt.

Thank you.

THE COURT: Thanks very much, Ms. Manca.

Okay. Picking a jury in COVID times is not easy. Judge Zilly did a jury trial where he lost several jurors to positive COVID tests, so that's why we went with 15, but now I feel like, ugh, I mean, I feel bad for the three alternates who may not get to deliberate. But, you know, the truth of the matter is, we needed it, and we still might need it, because anything can happen as deliberations start.

But the three alternates are Ms. XXXXXXXXXX, No. 15; Ms. XXXX, No. 9, and Mr. XXXXXXXXXXXX, No. 12. So you will not come back at 1:30 and start deliberating. You can go back to the jury room with your fellow jurors and say farewell, pick up any of your things.

The rest of you will be the 12 who will decide the case. But if anything were to happen to one, two, or three jurors during deliberations, you could still be substituted in, and the deliberations would begin anew. So all the talk about not doing any research or talking about the case still apply to those three alternates, also.

I would ask that you go back to Judge Zilly's courtroom for just a minute or two while Victoria then releases the three alternates, gets contact information, if she needs it, and then

we'll send you to lunch. So don't begin your deliberations until after you come back from lunch and are all together in Judge Zilly's courtroom. At that point, Victoria will have the Court's original instructions and will show you to how utilize the computer that's in there to look at evidence and exhibits.

You can leave your pens and jury instructions on your chair, including the alternates, because we'll take those, and we will let you know how things develop, for the alternates, to let you know where we are in the deliberations.

I've always told you you haven't heard anything or seen anything, well, now you've seen it all and heard it all, but don't start thinking about forming your conclusions about the case until you're all together in the jury room, and that's when the deliberations will begin. Okay?

All right. Victoria, do you want to take them over there?

And thank you so much to Ms. XXXXXXXX, Mr. XXXXXX, and Ms. XXXX. I hope you still enjoyed the process, even if it ends here. Thank you.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: All right. So when Victoria comes back, give her your phone numbers and reachability.

Ms. Thompson is going to stay with you?

MR. HAMOUDI: Yes, Your Honor.

THE COURT: Great.

And I've been doing this for a long time. We won't get a verdict this afternoon. We may get a question, though, so we need you available.

There's no way to predict when the jury will return a verdict, but I'm going to do it anyway. It won't be tomorrow morning. It will either be tomorrow afternoon or Tuesday morning. Remember, Monday is a holiday.

Ms. Thompson, you received absolutely superb representation from your lawyers. I hope you appreciate the fact that they worked so hard. You can see they put in so much personal care in presenting your case, so I hope you're proud of them.

THE DEFENDANT: Absolutely, I do, Your Honor.

THE COURT: Okay. Great.

Now, having said that, I'm going to say, Mr. Klein, just a tip for the future --

MR. KLEIN: Sorry.

THE COURT: No, no; no nodding your head during Mr. Hamoudi's closing argument.

And then Ms. Meister and Professor Halderman, no whispering during court, especially when the jury is looking right at you. It is rude.

Hang in there until Victoria comes back, and we'll get your information.

We'll be in recess.

(Court in recess 12:15 p.m. to jury release at 4:15 p.m.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 16th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter